

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application:

1 1. (Currently Amended) A communications network security method comprising:  
 2 identifying a plurality of routes that define ~~the~~ a first communications network;  
 3 identifying a plurality of hosts associated with the first communications network  
 4 as a function of the plurality of routes;  
 5 performing a census of the first communications network as a function of the  
 6 plurality of hosts to determine a topology of the first communications network;  
 7 probing at least one host of the plurality hosts of the first communications  
 8 network by transmitting a packet to the host, the host being selected from the census  
 9 results and the packet having at least a source address ~~determined as a function of the~~  
 10 ~~topology~~ which is associated with a second communications network; and  
 11 determining a security characteristic of the probed host as a function of a response  
 12 by the probed host in receiving the packet, the security characteristic being a measure of  
 13 connectivity between the first communications network and the second communications  
 14 network.

1 2. (Currently Amended) The method of claim 1 wherein the source address is an  
 2 IP address associated with a host external to the first communications network, and the  
 3 external host being associated with the second communications network ~~and the packet is~~  
 4 ~~constructed as a function of the source address and an IP address associated with the at~~  
 5 ~~least one host.~~

1 3. (Original) The method of claim 2 wherein the response of the probed host to  
 2 the receipt of the packet includes transmitting a second packet, the second packet being  
 3 derived using at least a portion of information from the received packet.

1 4. (Cancelled) ~~the performing the census operation further comprises:~~

2 ~~pinging a plurality of IP addresses to verify their respective validity, the plurality~~  
3 ~~of IP addresses being identified from the plurality of routes;~~  
4 ~~pinging particular hosts of the plurality of hosts to verify their respective location~~  
5 ~~in the topology of the communications network;~~  
6 ~~performing at least a first DNS lookup for at least one of the particular hosts; and~~  
7 ~~performing at least a second DNS lookup across a communications channel, the~~  
8 ~~communications channel serving to connect the communications network with a network~~  
9 ~~external to the communications network, the second DNS lookup identifying a specific~~  
10 ~~host of the plurality of hosts.~~

a1  
1 5. (Currently Amended) The method of claim 2 wherein the first  
2 communications network and the second communications network have different security  
3 levels, and the measure of connectivity is a function of whether the probed host of the  
4 first communications network communicates with the external host associated with the  
5 second communications network. The method of claim 3 wherein the probing the at least  
6 one host operation further comprises:  
7 identifying the IP address associated with the probed host from the census; and  
8 generating the packet as a function of the IP address associated with the probed  
9 host and the IP address associated with a host external to the communications network.

1 6. (Currently Amended) The method of claim 2-5 wherein the measure of  
2 connectivity is determining-determined the security characteristic operation further  
3 comprises by the further operation of:  
4 monitoring the probed host to determine the response, and if the response includes  
5 a transmission of a second packet from the probed host, generating a security alert  
6 message identifying the probed host as a security risk.

1 7. (Currently Amended) The method of claim 3 wherein the second packet is  
2 derived using at least a portion of information from the transmitted packet  
3 first communications network and the second communications network have different security  
4 levels.

1           8. (Currently Amended) The method of claim ~~7~~3 wherein the transmitted packet  
2 is a TCP packet which returns a TCP packet in response thereto.

1           9. (Currently Amended) The method of claim ~~8~~3 wherein the second packet is a  
2 UDP packet or an ICMP packet, which returns either a UDP packet or ICMP packet in  
3 response thereto.

1           10. (Currently Amended) A method for analyzing network security of a first  
2 communications network, the method comprising:

3           ~~identifying a plurality of routes that define the communications network;~~

4           ~~identifying a plurality of hosts internal to the communications network as a~~  
5 ~~function of the plurality of routes;~~

6           ~~performing receiving a census of the first communications network as a function~~  
7 ~~of the plurality of hosts to determine a topology of the communications network;~~

a' 8           transmitting a packet from a host ~~external to~~of the a second communications  
9 network to a particular one host of ~~the a~~ plurality of hosts internal to the first  
10 communications network, the internal host being selected from the census, and the packet  
11 being generated as a function of both an IP address associated with the host ~~external to~~of  
12 the second communications network and an IP address associated with the ~~particular one~~  
13 internal host of the plurality of hosts internal to ~~the~~of the first communications network;  
14 and

15           determining a security characteristic of the particular one internal host of the first  
16 communications network as a function of a response by the internal host to the receipt of  
17 the packet, the security characteristic being a measure of connectivity between the first  
18 communications network and the second communications network.

1           11. (Currently Amended) The method of claim 10 wherein the measure of  
2 connectivity is a function of whether the internal host of the first communications  
3 network communicates with the host of the second communications network, and the

4 ~~measure of connectivity being the determining the security characteristic operation~~  
5 ~~further comprises determined by the further operation of:~~

6 monitoring the ~~probed-internal~~ host to determine the response, and if the response  
7 includes a transmission of a second packet from the ~~probed-internal~~ host, generating a  
8 security alert message identifying the ~~probed-internal~~ host as a security risk.

1 12. (Original) The method of claim 11 wherein the second packet is derived  
2 using at least a portion of information from the transmitted packet.

1 13. (Cancelled) ~~the performing the census operation further comprises:~~  
2 ~~——pinging a plurality of IP addresses to verify their respective validity, the plurality~~  
3 ~~of IP addresses being identified from the plurality of routes;~~  
4 ~~——pinging particular hosts of the plurality of hosts to verify their respective location~~  
5 ~~in the topology of the communications network;~~  
6 ~~——performing at least a first DNS lookup for at least one of the particular hosts; and~~  
7 ~~——performing at least a second DNS lookup across a communications channel, the~~  
8 ~~communications channel serving to connect the communications network with a network~~  
9 ~~external to the communications network, the second DNS lookup identifying a specific~~  
10 ~~host of the plurality of hosts.~~

1 14. (Currently Amended) The method of claim 12 wherein the ~~probed-internal~~  
2 host is a dual-homed host.

1 15. (Currently Amended) The method of claim 11 wherein the security  
2 characteristic includes an indication that the ~~probed-internal~~ host is outside any security  
3 measures provided by a firewall associated with the first communications network.

1 16. (Currently Amended) A communications system comprising:  
2 a first plurality of computers associated with a first communications network;  
3 a second plurality of computers associated with a second communications  
4 network; and

5 a security host computer which determines a security characteristic of a first  
6 computer from the plurality of computers, the security characteristic being a measure of  
7 connectivity between the first communications network and the second communications  
8 network ~~performs a census of the communications network as a function of the first~~  
9 ~~plurality of computers, and by probes probing~~ the first computer by transmitting a packet  
10 to the first computer, the first computer being selected from ~~the a census results of the~~  
11 first communications network and the packet being generated as a function of both an IP  
12 address associated with a second computer of the second plurality of computers and an IP  
13 address associated with the first computer, and determining ~~a security level associated the~~  
14 measure of connectivity ~~with the first computer as a function of a response of the first~~  
15 computer to receiving the packet.

1 17. (Original) The communications system of claim 16 wherein the security host  
2 computer is associated with the first communications network.

ai  
1 18. (Currently Amended) The communications system of claim 17 wherein the  
2 response of the first computer to the receipt of the packet includes transmitting a second  
3 packet, the second packet being derived using at least a portion of information from the  
4 received packet.

1 19. (Currently Amended) The communications system of claim 18 wherein the  
2 security host computer determines the measure of connectivity ~~security characteristic by~~  
3 monitoring the probed first computer to determine the response, and if the response  
4 includes ~~a the~~ transmission of the second packet from the probed host, generating a  
5 security alert message identifying the first computer as a security risk.

1 20. (Amended) The communications system of claim 17 wherein the first  
2 communications network is an intranet and the second communications network is an  
3 Internet, and the first communications network and the second communications network  
4 have different security levels.

1 21. (Currently Amended) A security host computer comprising:

2 means for performing a census of a first communications network and  
3 determining a topology of ~~a~~ the first communications network, the topology being  
4 defined by at least one computer,

5 means for probing the at least one computer by transmitting a packet to the  
6 computer, the computer being selected from the census results and the packet being  
7 generated as a function of the topology, an IP address associated with a particular host  
8 computer associated with a second communications network and an IP address associated  
9 with the computer, the second communications network being separate from the first  
10 communications network; and

11 a monitor for determining a security level of the computer as a function of a  
12 response by the computer to the receipt of the packet, and the security level being a  
13 measure of connectivity between the first communications network and the second  
14 communications network.

a' 1 22. (Currently Amended) The security host computer of claim 21 wherein the  
2 measure of connectivity is determined by the monitor monitors monitoring the computer's  
3 ~~to determine the~~ response, and if the response includes a transmission of a second packet  
4 from the computer, a security alert message identifying the computer as a security risk is  
5 generated.

1 23. (Currently Amended) The security host computer of claim 22 wherein the  
2 ~~security level is determined with respect to a firewall located between the first~~  
3 ~~communications network and the second communications network~~ have different security  
4 levels.

1 24. (Currently Amended) A machine-readable medium having stored thereon a  
2 plurality of instructions, the plurality of instructions including instructions that, when  
3 executed by a machine, cause the machine to perform of a method for ~~identifying~~  
4 analyzing a first communications network's integrity ~~plurality of routes that define the~~  
5 ~~communications network; identifying a plurality of hosts as a function of the plurality of~~

6 ~~routes; performing by receiving~~ a census of the first communications network ~~as a~~  
7 ~~function of the plurality of hosts to determine a topology of the communications network;~~  
8 ~~probing at least one host of the plurality hosts~~ a host by transmitting a packet to the host,  
9 the host being selected from the census results and the packet being derived as a function  
10 of the ~~a~~ topology of the first communications network and the packet having a source  
11 address which is associated with a second communications network; and determining a  
12 ~~security characteristic of the probed host~~ the first communications network's integrity as  
13 a function of a response by the probed host in receiving the packet.

a1  
1 25. (Currently Amended) The machine-readable medium of claim 24 further  
2 ~~comprising instructions that, when executed by a machine, cause the machine to perform~~  
3 ~~the probing the at least one host operation by identifying the IP address associated with~~  
4 ~~the probed host from the census; and generating the packet as a function of the IP address~~  
5 ~~associated with the probed host and the IP address associated with a host external to the~~  
6 ~~communications network~~ wherein the response indicates a measure of connectivity  
7 between the first communications network communicates and the second  
8 communications network.

1 26. (Original) The machine-readable medium of claim 25 wherein the response of  
2 the probed host to the receipt of the packet includes transmitting a second packet, the  
3 second packet being derived using at least a portion of information from the received  
4 packet.

1 27. (Currently Amended) The machine-readable medium of claim 26 wherein the  
2 first communications network is an intranet, and the ~~external host is associated~~  
3 ~~with~~ second communications network is an Internet.

---